CLAIMS

1. High-performance specification resolution method characterized in that it comprises:

a) a step for formulating the audit conditions one wishes to detect using specification formulas expressing fraudulent entry or attack patterns or abnormal operations, this being non-limiting, to be verified by examining the records of the computer system's log file;

b) a step for expanding formulas into subformulas;

c) a step for scanning by an interpreter, which consists of generating, for each expanded formula in each record, Horn clauses to resolve in order to detect whether or not the formula is valid in this record, the Horn clauses expressing the implications resolvent of the subformulas for each record scanned, in positive clauses, i.e. counting only a positive literal, and in non-positive clauses, i.e. counting at least one negative literal, which negative literals form the negative part of the clause;

d) a step for the storing positive Horn clauses in a stack of worked subformulas, and a step for storing, in a table comprising a representation, the implicating subformula(s) constituting the negative part of the clause and the link with the implicated subformula(s) constituting the positive part of the clause, and storing in a counter the number of formulas or subformulas present in the negative part of the clause for each implicated subformula;

e) a step for resolving the table based on each positive clause encountered, so as to generate either an output file or an action of the computer system;

f) a step for iterating steps b) through e) until the scanning of all the records in the log file is complete.

2. Method according to claim 1, characterized in that a temporal logic is used for the formulation of the specification.

3. Method according to claim 1, characterized in that the table is a matrix and is indexed in columns by the subscripts of the formulas appearing in the negative part of the Horn clauses, and the lines are the Horn clauses exactly.

4. Method according to claim 1, characterized in that the table is preferably

represented in the form of a sparse matrix, the columns being represented by means of chained lists and the lines remaining implicit.

5. Method according to claim 1 or 2, characterized in that a step for optimizing the expansion of the formulas is obtained through a hash table in order to ensure that the same formula is not expanded more than once in each record.

6. Method according to claim 1, characterized in that the log file is scanned only once from beginning to end.

7. Computer system comprising storage means and means for executing programs for implementing the method according to any of claims 1 through 6, characterized in that the system comprises:

- an adapting means for translating the information from the log file formulated in the specific language of the machine into a language comprehensible to an interpreting means;
- the interpreting means receiving the information from the adapter and receiving the formulation of the specification in the temporal logic in a specification formula in order to expand this formula and fill in the table and the stack of worked subformulas stored in a memory of the computer system and resulting from the scanning of the computer system's log file;
- a clause processing algorithm executed by the computer system, which makes it possible to resolve the Horn clauses using the information from the table and the stack of worked subformulas, this clause processing algorithm generating an output file or generating an action.